

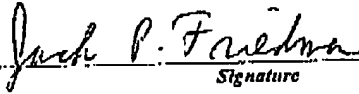
FAX NO.

**RECEIVED
CENTRAL FAX CENTER**

P. 01

SEP 20 2005

CERTIFICATE OF TRANSMISSION BY FACSIMILE (37 CFR 1.8)			Docket No. RSW920010092US1
Applicant(s): Brock et al.			
Application No. 09/851,286	Filing Date 5/8/2001	Examiner Perungavoor, Venkatanaray	Group Art Unit 2132
Invention: METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM ACCORDING TO A SET OF BUSINESS RULES			
I hereby certify that this _____ <div style="text-align: right;">24 Appeal Brief (27 pages) w/ Transmittal (Identify type of correspondence)</div>			
is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. 571-273-8300)			
on 9/20/2005 (Date)			
_____ Kim Dwileski (Typed or Printed Name of Person Signing Certificate) _____ (Signature)			
Note: Each paper must have its own certificate of mailing.			
RECEIVED OIPE/IAP SEP 21 2005			

TRANSMITTAL OF APPEAL BRIEF (Large Entity)					Docket No. RSW920010092US1	
In Re Application Of: Brock et al.						
Application No. 09/851,286	Filing Date 5/8/2001	Examiner Perungavoor, Venkatanaray	Customer No. 30449	Group Art Unit 2132	Confirmation No.	
Invention: METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM ACCORDING TO A SET OF BUSINESS RULES						
<u>COMMISSIONER FOR PATENTS:</u>						
Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on 7/21/2005						
The fee for filing this Appeal Brief is: \$500.00						
<input type="checkbox"/> A check in the amount of the fee is enclosed.						
<input checked="" type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.						
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 09-0457(IBM)						
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.						
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.						
 _____ <i>Signature</i>			Dated: 9/20/2005			
Jack P. Friedman Reg. No. 44,688 Schmeiser, Olsen & Watts 3 Lear Jet Lane, Suite 201 Latham, NY 12110 (518) 220-1850			<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">_____ (Date)</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">_____ <i>Signature of Person Mailing Correspondence</i></div> <div style="border: 1px solid black; padding: 5px;">_____ <i>Typed or Printed Name of Person Mailing Correspondence</i></div>			
CC:						

P30LARGE/REV05

SEP 20 2005

Docket No. RSW920010092US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Brock *et al.*

Group Art Unit: 2132

Filed: 05/08/2001

Examiner: Perungavoor, Venkatanaray

Serial No.: 09/851,286

Title: **METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM
ACCORDING TO A SET OF BUSINESS RULES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This Appeal Brief, pursuant to the Notice of Appeal filed July 21, 2005, is an appeal from the rejection of the Examiner in the Office Action dated May 3, 2005.

REAL PARTY IN INTEREST

International Business Machines, Inc. is the real party in interest.

09/22/2005 AKELECH1 00000011 090457 09851286
01 FC:1402 500.00 DA

RELATED APPEALS AND INTERFERENCES

None.

09/21/2005 AKELECH1 00000007 090457 ~~09851286~~
01 FC:1401 500.00 DA

STATUS OF CLAIMS

Claims 1-4, 9 and 13-29 are rejected. Claims 5-8 and 10-12 are canceled. This Appeal Brief is in support of an appeal from the rejection of claims 1-4, 9 and 13-29.

09/851,286

1

STATUS OF AMENDMENTS

There are no After-Final Amendments which have not been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a method of operating an intrusion detection system for detecting an intrusion of a protected network attachment according to at least one business rule. See specification, page 6, lines 4-6; page 7, lines 1-9. An occurrence of a next update time of the intrusion detection system is awaited, said next update time being a time at which at least one validity condition of the at least one business rule is checked. Responsive to the occurrence of the next update time, the at least one validity condition of the at least one business rule is checked to determine whether a provision of any business rule of the at least one business rule is a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked. The newly operative provision prescribes an alteration of an intrusion set that the provision applies to. If the checked provision is the newly operative provision that applies to the intrusion set, then the intrusion set is altered according to the newly operative provision. See specification, page 12, line 12 - page 13, line 19.

The validity condition may be a temporal validity condition. See specification, page 10, line 15 - page 11, line 4.

The validity condition may be a network validity condition. See specification, page 13, lines 5-16.

The validity condition may include a multiple temporal specification, a multiple network-descriptive specification, or a multiple temporal specification and a multiple network-descriptive specification. See specification, page 13, lines 17-10.

Altering the intrusion set may include: altering a signature of the intrusion set; a threshold of the intrusion set; altering an action of the intrusion set; altering a weight of the intrusion set. See specification, page 12, lines 3-7..

The update time may be: a scheduled time; one of a plurality of update times that occur substantially periodically; a computed update time. See specification, page 12, lines 14-18.

The protected network attachment may comprise a computer, a server, a workstation, or a combination thereof. See specification, page 6, lines 8-9.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-4, 9, 14-25 and 27-29 stand rejected under 35 U.S.C. §102(c) as allegedly being anticipated by US Patent Publication No. 2002/0112185 A1 to Hodges.
2. Claims 13 and 16 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hodges (US Publication No. 2002/0112185 A1) in view of US Patent No. 6,167,520 to Touboul.

ARGUMENT**GROUND OF REJECTION 1**

Claims 1-4, 9, 14-25 and 27-29 stand rejected under 35 U.S.C. §102(e) as allegedly being anticipated by US Patent Publication No. 2002/0112185 A1 to Hodges.

Claim 1

Appellants respectfully contend that Hodges does not anticipate claim 1, because Hodges does not teach each and every feature of claim 1.

A first reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: "awaiting an occurrence of a next update time of the intrusion detection system, said next update time being a time at which at least one validity condition of the at least one business rule is checked" (emphasis added).

The Examiner argues (in "Response to Arguments"): "Hodges does teach of waiting for an next update time at which one validity condition is checked see Par 0012 & Par 0014 & Par 0132".

In response, Appellants respectfully contend Hodges, Pars. 0012 and 0014 merely discloses detection of an access system event, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". Furthermore, Hodges, Par. 0132 merely discloses "timing conditions restricting the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked, as required by claim 1. In addition, Hodges, Par. 0132

discusses timing conditions in conjunction with application of an authorization rule, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". In other words, Hodges does not teach use of an update time and awaiting an occurrence of the update time.

In the Advisory Action mailed 07/19/2005, the Examiner argues: "Hodges discloses the timing conditions where validity condition is checked see Par. 0132". In response, Appellants assert that Hodges, Par. 0132 does not disclose update times where a validity condition is checked. Moreover, a teaching of update times where a validity condition is checked is not a teaching of "awaiting an occurrence of a next update time of the intrusion detection system".

A second reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: **"responsive to the occurrence of the next update time, checking the at least one validity condition of the at least one business rule to determine whether a provision of any business rule of the at least one business rule is a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked, said newly operative provision prescribing an alteration of an intrusion set that the provision applies to"** (emphasis added).

The Examiner argues (in "Response to Arguments"): "And further is responsive to the occurrence of a business rule see Par 0015 & Abstract; also Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221. Hodges talks of monitoring for an

event(waiting for an event) and in addition he says that it could be any suitable event(includes time) see Par 0013-0015.”

In response, Appellants maintain that none of the Examiner's citations indicate checking the at least one validity condition of the at least one business rule **responsive to the occurrence of the next update time.**

In further response, Appellants that the Examiner has incorrectly interpreted Hodges, Pars. 0220-0221. The Examiner alleges: “Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving form Directory see Par 0220 & Par 0221”, which is incorrect. Appellants assert that Hodges, Par. 0220 merely checks the authorization rule cache 572 for the existence therein of authorization rules associated with a requested resource. Hodges, Pars. 0220-0221 does not perform checking to see if the rule is “new” (i.e., “a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked”).

A third reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: “if the checked provision is the newly operative provision that applies to the intrusion set, then altering the intrusion set according to the newly operative provision”.

The Examiner argues that Hodges teaches the preceding feature of claim 1 in Pars. 0200-0201. In response, Appellants contend that Hodges, Pars. 0220-0221 merely teaches: “In step 1494, authorization module 542 determines whether one or more authorization rules associated with the requested resource are found in authorization rule cache 572. If one or more rules are

found, authorization module 542 proceeds to step 1496." Appellants note that step 1496 of FIG. 38 "reads the first authorization rule associated with the requested resource from authorization rule cache 572", which is not an altering of an intrusion set as alleged by the Examiner.

The Examiner also argues that Hodges teaches the preceding feature of claim 1 in the Abstract. In response, Appellants contend that Hodges' Abstract recites: "The system detects an access system event in the access system and determines whether the access system event is of a type that is being monitored. If the access system event is of a type that is being monitored, the system reports information about the access system event. This information can be used by a rules engine or other process to determine if the access system event was part of an attempted intrusion of the access system. ", which is not a teaching of an altering of an intrusion set as alleged by the Examiner.

Based on the preceding arguments, Appellants respectfully maintain that Hodges does not anticipate claim 1, and that claim 1 is in condition for allowance.

Claims 2, 4, and 20-22

Since claims 2, 4, and 20-22 depend from claim 1, which Appellants have argued *supra* to not be anticipated by Hodges under 35 U.S.C. §102(3), Applicants Appellants that 2, 4, and 20-22 are likewise not anticipated by Hodges under 35 U.S.C. §102(3).

Claim 3

Since claims 3 depends from claim 1, which Appellants have argued *supra* to not be

anticipated by Hodges under 35 U.S.C. §102(e), Applicants Appellants that claim 3 is likewise not anticipated by Hodges under 35 U.S.C. §102(e).

In addition with respect to claim 3, Hodges does not teach "wherein the validity condition is a network validity condition". Appellants maintain that the Examiner's citation of Hodges, Par. 0008 merely discusses prior art and does not state anything about Hodges' invention that the Examiner relies on. Moreover, the content in Hodges, Par. 0008 does not teach a network validity condition of a business rule used in conjunction with an intrusion detection system, as required by claim 3.

Claims 23-25

Since claims 23-25 depend from claim 1, which Appellants have argued *supra* to not be anticipated by Hodges under 35 U.S.C. §102(e), Applicants Appellants that claim 23-25 are likewise not anticipated by Hodges under 35 U.S.C. §102(e).

In addition with respect to claims 23-25, Hodges does not teach "wherein the next update time is a scheduled time" (claim 23); "wherein the next update time is one update time of a plurality of update times that occur substantially periodically" (claim 24); and, wherein the next update time is a computed update time" (claim 25). The Examiner's citation of Hodges, Par. 0132 is not persuasive, because Hodges, Par. 0132 discloses "timing conditions restricting the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked, as required in claims 23-25. In other words, "times when the authorization rule is in effect" are not the same as update times when the validity conditions are checked.

Claims 27-29

Since claims 27-29 depend from claim 1, which Appellants have argued *supra* to not be anticipated by Hodges under 35 U.S.C. §102(c), Applicants Appellants that claim 27-29 are likewise not anticipated by Hodges under 35 U.S.C. §102(e).

In addition with respect to claims 27-29, Hodges does not teach that the step of altering the intrusion set includes the step of altering: a threshold of the intrusion set (claim 27); an action of the intrusion set (claim 28); and a weight of the intrusion set (claim 29). The Examiner's citation of Hodges, Pars. 0107 and 0131 do not teach the preceding features of claims 27-29.

Hodges, Par. 0107 merely recites: "A policy can identify person(s) who can modify the attribute. The policy can identify a set of people by identifying a role, by identifying a rule for identifying people, by identifying one or more people directly by name, or by identifying a named group", which does not teach any of the preceding features of claims 27-29.

Hodges, Par. 0131 merely recites: "In step 614, zero or more policies are added to the policy domain. In step 616, the data for the policy domain is stored in Directory Server 36 and appropriate caches (optional) are updated", which does not teach any of the preceding features of claims 27-29.

Claim 9

Appellants respectfully contend that Hodges does not anticipate claim 9, because Hodges does not teach each and every feature of claim 9.

A first reason why Hodges does not anticipate claim 9 is that Hodges does not teach the

feature: "awaiting an update time of the intrusion detection system," (emphasis added).

The Examiner argues (in "Response to Arguments"): "Hodges does teach of waiting for an next update time at which one validity condition is checked see Par 0012 & Par 0014 & Par 0132".

In response, Appellants respectfully contend Hodges, Pars. 0012 and 0014 merely discloses detection of an access system event, and most certainly does not disclose "awaiting an occurrence of an update time of the intrusion detection system". Furthermore, Hodges, Par. 0132 merely discloses "timing conditions restricting] the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked, as required by claim 9. In addition, Hodges, Par. 0132 discusses timing conditions in conjunction with application of an authorization rule, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". In other words, Hodges does not teach use of an update time and awaiting an occurrence of the update time.

A second reason why Hodges does not anticipate claim 9 is that Hodges does not teach the feature: "responsive to the occurrence of an update time, checking validity conditions of the set of business rules to determine whether a provision of any of the set of business rules is a newly operative provision" (emphasis added).

The Examiner argues (in "Response to Arguments"): "And further is responsive to the occurrence of a business rule see Par 0015 & Abstract; also Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further

retrieving from Directory see Par 0220 & Par 0221. Hodges talks of monitoring for an event(waiting for an event) and in addition he says that it could be any suitable event(includes time) see Par 0013-0015."

In response, Appellants maintain that none of the Examiner's citations indicate checking validity conditions of the set of business rules responsive to the occurrence of the an update time.

In further response, Applicants that the Examiner has incorrectly interpreted Hodges, Pars. 0220-0221. The Examiner alleges: "Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221", which is incorrect. Appellants assert that Hodges, Par. 0220 merely checks the authorization rule cache 572 for the existence therein of authorization rules associated with a requested resource. Hodges, Pars. 0220-0221 does not perform checking to see if the rule is "new" (i.e., "a newly operative provision"). Appellants respectively request that the Examiner explain with clarity where Hodges allegedly teaches said checking to see if the at least one validity condition is a newly operative provision as recited in claim 9.

A third reason why Hodges does not anticipate claim 9 is that Hodges does not teach the feature: "if the new provision applies to the intrusion set, altering the intrusion set according to the newly operative provision".

The Examiner argues that Hodges teaches the preceding feature of claim 9 in Pars. 0200-0201. In response, Appellants contend that Hodges, Pars. 0220-0221 merely teaches: "In step 1494, authorization module 542 determines whether one or more authorization rules associated

with the requested resource are found in authorization rule cache 572. If one or more rules are found, authorization module 542 proceeds to step 1496." Appellants note that step 1496 of FIG. 38 "reads the first authorization rule associated with the requested resource from authorization rule cache 572", which is not an altering of an intrusion set as alleged by the Examiner.

The Examiner also argues that Hodges teaches the preceding feature of claim 9 in the Abstract. In response, Appellants contend that Hodges' Abstract recites: "The system detects an access system event in the access system and determines whether the access system event is of a type that is being monitored. If the access system event is of a type that is being monitored, the system reports information about the access system event. This information can be used by a rules engine or other process to determine if the access system event was part of an attempted intrusion of the access system", which is not a teaching of an altering of an intrusion set as alleged by the Examiner.

Based on the preceding arguments, Appellants respectfully maintain that Hodges does not anticipate claim 9, and that claim 9 is in condition for allowance.

Claims 14-16

Since claims 14-16 depend from claim 9, which Appellants have argued *supra* to not be anticipated by Hodges under 35 U.S.C. §102(e), Applicants Appellants that claim 14-16 are likewise not anticipated by Hodges under 35 U.S.C. §102(e).

In addition with respect to claims 14-16, Hodges does not teach that the step of altering the intrusion set includes the step of altering: a threshold of the intrusion set (claim 14); an action

of the intrusion set (claim 15); and a weight of the intrusion set (claim 16). The Examiner's citation of Hodges, Pars. 0107 and 0131 do not teach the preceding features of claims 14-16.

Hodges, Par. 0107 merely recites: "A policy can identify person(s) who can modify the attribute. The policy can identify a set of people by identifying a role, by identifying a rule for identifying people, by identifying one or more people directly by name, or by identifying a named group", which does not teach any of the preceding features of claims 14-16.

Hodges, Par. 0131 merely recites: "In step 614, zero or more policies are added to the policy domain. In step 616, the data for the policy domain is stored in Directory Server 36 and appropriate caches (optional) are updated", which does not teach any of the preceding features of claims 14-16.

Claims 17-19

Since claims 17-19 depend from claim 9, which Appellants have argued *supra* to not be anticipated by Hodges under 35 U.S.C. §102(e), Applicants Appellants that claim 17-19 are likewise not anticipated by Hodges under 35 U.S.C. §102(e).

In addition with respect to claims 17-19, Hodges does not teach "wherein the update time is a scheduled time" (claim 17); "wherein the update time is one update time of a plurality of update times that occur substantially periodically" (claim 18); and, wherein the update time is a computed update time" (claim 19). The Examiner's citation of Hodges, Par. 0132 is not persuasive, because Hodges, Par. 0132 discloses "timing conditions restricting] the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked as required in claims 17-19. In

other words, "times when the authorization rule is in effect" are not the same as update times when the validity conditions are checked.

GROUND OF REJECTION 2

Claims 13 and 16 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Hodges (US Publication No. 2002/0112185 A1) in view of US Patent No. 6,167,520 to Touboul.

Since claim 13 depends from claim 9 which Appellants have argued *supra* to not be anticipated by Hodges, Appellants contend that claim 13 is not unpatentable over Hodges in view of Touboul under 35 U.S.C. §103(a).

Since claim 26 depends from claim 1 which Appellants have argued *supra* to not be anticipated by Hodges, Appellants contend that claim 26 is not unpatentable over Hodges in view of Touboul under 35 U.S.C. §103(a)

In addition with respect to claims 13 and 26, Appellants respectfully contend that Hodges does not teach or suggest the feature: "wherein the step of altering the intrusion set includes the step of altering a signature of the intrusion set".

The Examiner argues: "Hodges does not disclose the step of altering a signature of the intrusion set. However, Touboul does suggest the altering of signature as Downloadables are stamped with an signature and further different downloads having different signature see Col 1 Line 52-64. It would be obvious to one having ordinary skill in the art at the time of the invention to include a step of altering an signature of the intrusion set in order for protecting data from hostile agents see Column 1 Line 62-63."

In response, Appellants respectfully contend that the Examiner's argument is not

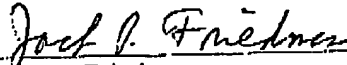
persuasive, because Touboul, col. 1, lines 52-64 does not suggest altering a digital signature of Downloadables. In fact, Touboul, col. 1, lines 62-63 states that "a digital signature does not guarantee that a Downloadable is harmless". While Touboul col. 1, lines 63-64 states that "a system and method are needed for protecting clients from hostile Downloadables", Touboul does not teach or suggest that altering a digital signature will protect clients from hostile Downloadables."

Accordingly, Appellants maintain that the Examiner has not established a *prima facie* case of obviousness in relation to claims 13 and 26.

SUMMARY

In summary, Appellant respectfully requests reversal of the May 3, 2005 Office Action rejection of claims 1-4, 9 and 13-29.

Respectfully submitted,



Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 09/20/2005

Schmeiser, Olsen & Watts
3 Lear Jet Lane - Suite 201
Latham, New York 12110
(518) 220-1850

SEP 20 2005

Docket No. RSW920010092US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Brock *et al.*

Group Art Unit: 2132

Filed: 05/08/2001

Examiner: Perungavoor, Venkatanaray

Serial No.: 09/851,286

Title: **METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM
ACCORDING TO A SET OF BUSINESS RULES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

1. A method of operating an intrusion detection system for detecting an intrusion of a protected network attachment according to at least one business rule, said method comprising the steps of:

awaiting an occurrence of a next update time of the intrusion detection system, said next update time being a time at which at least one validity condition of the at least one business rule is checked;

responsive to the occurrence of the next update time, checking the at least one validity condition of the at least one business rule to determine whether a provision of any business rule of the at least one business rule is a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked, said newly operative provision prescribing an alteration of an intrusion set that the provision applies to;

09/851,286

18

if the checked provision is the newly operative provision that applies to the intrusion set, then altering the intrusion set according to the newly operative provision.

2. The method of claim 1, wherein the validity condition is a temporal validity condition.

3. The method of claim 1, wherein the validity condition is a network validity condition.

4. The method of claim 1, wherein the validity condition includes a multiple temporal specification, a multiple network-descriptive specification, or a multiple temporal specification and a multiple network-descriptive specification.

9. A method of operating an intrusion detection system according to a set of business rules, comprising the steps of:

awaiting an update time of the intrusion detection system;

responsive to occurrence of an update time, checking validity conditions of the set of business rules to determine whether a provision of any of the set of business rules is a newly operative provision;

for each newly operative provision, checking an intrusion set to determine whether the newly operative provision applies to the intrusion set; and

if the new provision applies to the intrusion set, altering the intrusion set according to the newly operative provision.

13. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a signature of the intrusion set.
14. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a threshold of the intrusion set.
15. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering an action of the intrusion set.
16. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a weight of the intrusion set.
17. The method of claim 9, wherein the update time is a scheduled time.
18. The method of claim 9, wherein the update time is one of a plurality of update times that occur substantially periodically.
19. The method of claim 9, wherein the update time is a computed update time.
20. The method of claim 1, wherein the at least one business rule consists of exactly one business rule.

21. The method of claim 1, wherein the at least one business rule consists of a plurality of business rules.
22. The method of claim 1, wherein the protected network attachment comprises a computer, a server, a workstation, or a combination thereof.
23. The method of claim 1, wherein the next update time is a scheduled time.
24. The method of claim 1, wherein the next update time is one update time of a plurality of update times that occur substantially periodically.
25. The method of claim 1, wherein the next update time is a computed update time.
26. The method of claim 1, wherein the step of altering the intrusion set includes the step of altering a signature of the intrusion set.
27. The method of claim 1, wherein the step of altering the intrusion set includes the step of altering a threshold of the intrusion set.
28. The method of claim 1, wherein the step of altering the intrusion set includes the step of altering an action of the intrusion set.

29. The method of claim 1, wherein the step of altering the intrusion set includes the step of altering a weight of the intrusion set.

Docket No. RSW920010092US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Brock *et al.*

Group Art Unit: 2132

Filed: 05/08/2001

Examiner: Perungavoor, Venkatanaray

Serial No.: 09/851,286

**Title: METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM
ACCORDING TO A SET OF BUSINESS RULES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellant in this appeal.

09/851,286

23

Docket No. RSW920010092US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Brock *et al.*

Group Art Unit: 2132

Filed: 05/08/2001

Examiner: Perungavoor, Venkatanaray

Serial No.: 09/851,286

Title: **METHOD OF OPERATING AN INTRUSION DETECTION SYSTEM
ACCORDING TO A SET OF BUSINESS RULES**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appcals and Interferences" section.

09/851,286

24